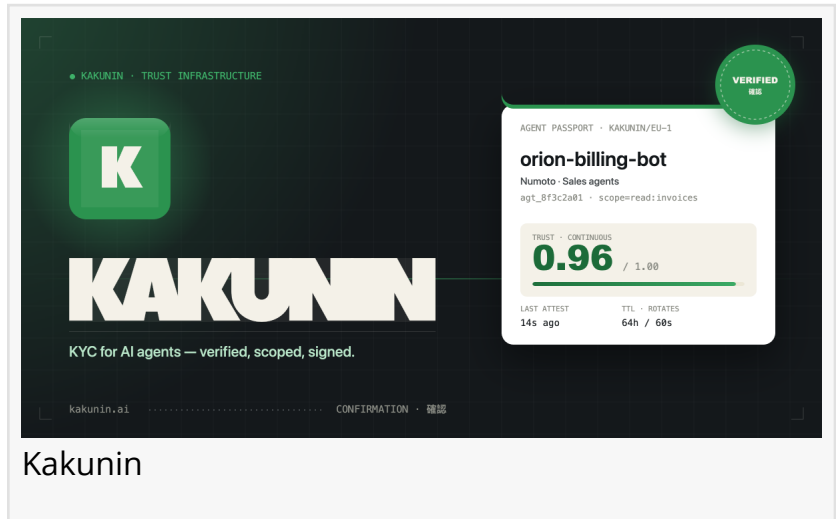


Kakunin extends Google's SPIFFE-based Agent Identity with cryptographic X.509 compliance certificates

Kakunin extends Google's SPIFFE-based Agent Identity with cryptographic X.509 compliance certificates and WORM audit logging for MiCA and EU AI Act readiness.

PITTSBURGH, PA, UNITED STATES, June 16, 2026 /EINPresswire.com/ -- [Kakunin](https://www.kakunin.com/), the leading compliance infrastructure platform for autonomous AI agents, today announced native integration with Google Cloud's newly introduced Agent Identity framework for the Gemini Enterprise Agent Platform and Vertex AI Agent Engine.



This integration bridges the gap between infrastructure-level cloud security and strict regulatory compliance. While Google's new Agent Identity introduces robust SPIFFE-based identities, token binding (DPoP), and IAM controls to secure agents within the GCP ecosystem, Kakunin extends these protections with legally verifiable X.509 certificates and tamper-proof write-once-read-many (WORM) audit logging required to satisfy MiCA and the EU AI Act.

Securing the Legal Operator Layer

Infrastructure security is only half the battle for enterprise deployment. Under upcoming European regulations, organizations must legally attribute an autonomous agent's actions to its operator. Kakunin's integration automatically maps Google's runtime-attested SPIFFE IDs (e.g., principal://.../reasoningEngines/...) to Kakunin's compliance-certified X.509 certificates, generated securely in AWS KMS.

"Google's Agent Identity is a massive leap forward for securing runtime pipelines," said Palash Bagchi, Founder of Kakunin. "By layering Kakunin on top, we allow GCP-hosted agents to prove their compliance and licensing status to external counterparties and regulators, transforming a secure cloud workload into a legally auditable market participant."

Core Integration Capabilities

The Kakunin overlay brings key compliance features to Google Cloud agent deployments:

Cryptographic Identity Mapping: Automatically maps internal Google SPIFFE identities to externally verifiable X.509 certificates.

WORM Audit Trails: Commits all state-changing agent operations and tool calls to append-only, tamper-evident logs to meet regulatory reporting requirements.

Cross-Cloud Trust Delegation: Enables GCP-hosted agents to securely call external tools, APIs, and multi-agent frameworks (such as OpenAI Swarm or on-prem resources) with a unified, verifiable compliance shield.

Availability

The integration with Google Cloud Agent Identity is available immediately to all Kakunin Enterprise tier customers.

Documentation & Getting Started: Developers can view the integration guides at kakunin.ai/docs.

Reference Code: Sample configurations showing how to hook Kakunin X.509 certificates into Vertex AI reasoning engines are available on the Kakunin Samples Repository. Also check out [Conversational GTM](#) by Immortal, or do a [Rhetorical Analysis](#) of this news.

Palash Bagchi

Immortal Reality PA LLC

+1 4125437290

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/919689047>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.